

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

First Named Inventor:	:	
Adam R. Schran	:	
	:	
Conf. No.: 3079	:	Group Art Unit: 2161
	:	
Appln. No.: 09/820,054	:	Examiner: Etienne Pierre Leroux
	:	
Filing Date: March 28, 2001	:	Attorney Docket No.: 10397-1U1
	:	
Title:	:	SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA

**AMENDED APPEAL BRIEF (37 C.F.R. § 41.37)**

This brief is being filed in response to the “Order Returning Undocketed Appeal” to Examiner mailed December 5, 2007. The fees required under § 41.20 were paid when the original Appeal Brief was filed and no additional fees are believed to be due.

In telephone calls held between Appellants’ undersigned representative and Examiner Leroux on December 10 and 11, 2007, it was agreed that Appellants would first file an Amended Appeal Brief that addresses the items highlighted in the Order, the Examiner will respond with an Amended Examiner’s Answer that clearly identifies the new grounds of rejection which relate only to dependent claims, and that Appellants would respond with an Amended Reply Brief that is identical in content to the originally filed Reply Brief, and that no request would be made to reopen prosecution in view of the new grounds of rejection.

In this Amended Reply Brief, the headings on pages 5, 10 and 12 now match grounds of rejection listed on page 5, and the two § 1.131 Declarations filed during prosecution are now included in Section IX, along with a statement setting forth where in the record that evidence was entered and considered by the Examiner.

I.	REAL PARTY IN INTEREST.....	3
II.	RELATED APPEALS AND INTERFERENCES.....	3
III.	STATUS OF CLAIMS.....	3
IV.	STATUS OF AMENDMENTS.....	3
V.	SUMMARY OF CLAIMED SUBJECT MATTER.....	3
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL.....	5
VII.	ARGUMENTS – REJECTIONS UNDER 35 U.S.C. § 103.....	5
	A. There is a clear error in the Examiner’s Final Rejection of claims 1, 7, 12, 16, 22 and 27 because Walker et al. in view of Shrader do not disclose or suggest any of the steps (a)-(c) of claims 1 and 16, at least step (c) of claims 7 and 22, and at least step (a) of claims 12 and 27.....	5
	B. Summary of claim limitations in claims 1, 7, 12, 16, 22 and 27 that are not disclosed or suggested by Walker et al. in view of Shrader.....	10
	C. Patentability of dependent claims 2, 4-6, 8-11, 13-15, 17, 19-21, 23-26 and 28-30 over Walker in view of Shrader; and Patentability of dependent claims 3 and 18 over Walker in view of Shrader and NIS 2000.....	12
	D. Applicants’ arguments do not stand or fall based on application of the CAFC’s nonobviousness doctrine using a motivation/suggestion/teaching test.....	12
	E. Conclusion.....	13
VIII.	APPENDIX OF CLAIMS.....	14
IX.	APPENDIX OF EVIDENCE.....	22
X.	APPENDIX OF RELATED DECISIONS.....	22
XI.	OTHER MATERIAL THAT APPELLANT CONSIDERS NECESSARY OR DESIRABLE.....	22

## **I. REAL PARTY IN INTEREST**

This application is assigned to Ascentive LLC, by an Assignment recorded on March 28, 2001, at Reel No. 011662, Frame 0557. Accordingly, Ascentive LLC is the real party in interest.

## **II. RELATED APPEALS AND INTERFERENCES**

Appellants, their Assignee and their legal representatives are unaware of the existence of any related appeals and/or interferences that will directly affect, be directly affected by, or have a bearing on the decision in the pending appeal.

## **III. STATUS OF CLAIMS**

Claims 1-30 are pending in the instant application on appeal.

Claims 1-30 stand twice rejected as discussed below and are the subject of the instant appeal. The grounds of rejection in the Final Office Action dated November 21, 2006 were unclear. Accordingly, Applicants' undersigned representative telephoned the Examiner on December 7, 2006 to request clarification of the grounds. The Examiner stated that the § 102(e) rejection over U.S. Patent Application Publication No. 2002/0055912 (Buck) was withdrawn, and that the only outstanding rejections are based on Walker et al. in view of Shrader, and Walker et al. in view of Shrader and Julien Jay (Norton Internet Security 2000). The Examiner further stated that all pending claims are rejected over these combinations of references, even though the grounds of rejection on page 2 of the Office Action only refers to claims 1, 2 and 4-6.

The complete text of claims 1-30, as pending, is attached hereto in Appendix VIII.

## **IV. STATUS OF AMENDMENTS**

No amendments were filed in the present application subsequent to the Final Rejection.

## **V. SUMMARY OF CLAIMED SUBJECT MATTER**

The following summary describes one preferred embodiment of the present invention. The scope of the present invention is not limited to the specific configuration or elements shown in the figures and described below.

Independent claim 1 recites a method of screening cookie files in a client machine (20), wherein a cookie file includes a cookie file source (page 3, lines 2-4; page 5, lines 18-19 and

28-29; page 7, lines 24-26; a cookie file source is an attribute of a cookie file, and thus it is inherent that a cookie file includes a cookie file source). A request from a subscriber is received at a server to send a list of cookie file sources to the client machine (page 6, lines 1-4 and Fig. 1). The list of cookie file sources is then downloaded from the server to the client machine (page 6, lines 1-4 and Fig. 1). The downloaded list of cookie file sources is then used to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list (page 8, lines 15-17; page 9, lines 15-20; block 60 of Fig. 3).

Independent claim 7 recites a method of creating a composite list of cookie file sources in a client machine (page 5, lines 25-28; page 6, lines 8-14). A first exception list is created that includes the identity of cookie file sources that are permitted to store cookie files in the client machine (personal trustlist 16 shown in Figs. 1, 3, 5 and 6). A cookie file includes a cookie file source (page 3, lines 2-4; page 5, lines 18-19 and 28-29; page 7, lines 24-26; a cookie file source is an attribute of a cookie file, and thus it is inherent that a cookie file includes a cookie file source). A second exception list is created that includes the identity of cookie file sources that are not permitted to store cookie files in the client machine (personal blacklist 18 shown in Figs. 1, 3, 5 and 6). A master list of cookie file sources is received at the client machine from a service provider (page 6, lines 1-4). The master list is then modified in accordance with the first and second exception lists, wherein the composite list is the modified master list (page 5, lines 25-28; page 6, lines 8-14).

Independent claim 12 recites another method of creating a composite list of cookie file sources in a client machine (page 5, lines 25-28; page 6, lines 8-14). A master list of cookie file sources is received at the client machine from a service provider (page 6, lines 1-4). Cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine are deleted (page 5, lines 25-28; page 6, lines 8-14). Cookie file sources are added to the master list that correspond to one or more untrusted cookie file sources listed in the client machine (page 5, lines 25-28; page 6, lines 8-14). The composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources (page 5, lines 25-28; page 6, lines 8-14).

Independent claims 16, 22 and 27 recite article of manufacture versions of claims 1, 7 and 12, respectively. Support for the article of manufacture limitation is provided on page 10,

lines 20-24.

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Claims 1, 2, 4-17 and 19-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker et al. (hereafter, “Walker”) in view of Shrader.

Claims 3 and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker in view of Shrader and Julien Jay (Norton Internet Security 2000).

As discussed above, the Examiner clarified that all pending claims are rejected over these combinations of references, even though the grounds of rejection on page 2 of the Office Action only refers to claims 1, 2 and 4-6.

## **VII. ARGUMENTS – REJECTIONS UNDER 35 U.S.C. § 103**

A. There is a clear error in the Examiner’s Final Rejection of claims 1, 7, 12, 16, 22 and 27 because Walker in view of Shrader do not disclose or suggest any of steps (a)-(c) of claims 1 and 16, at least step (c) of claims 7 and 22, and at least step (a) of claims 12 and 27

### **i. Background to Applicants’ Invention**

The following text portion from page 2, lines 19-30 of the present specification highlights one of the deficiencies in the prior art that the presently claimed invention addresses:

There are software programs that let users create a profile of which types of cookie files they will accept. However, there is no guarantee that cookie files generated by companies with a history of abusing the use of cookie files will be screened out, nor is there a universal reference source for determining which cookie file sources should not be accepted. What is needed is a professional service that constantly researches and evaluates cookie file sources (e.g., websites), cookie files, consumer complaints and other statistical data, and develops and electronically distributes to subscribing computer users, on a periodic basis, a list of those cookie file sources that the service recommends should not be permitted to store cookie files in the subscribing user's computer. What is also needed is a user-friendly interface for enabling a user to easily and automatically modify the distributed list once it is received by the user's computer, such that the user may customize the list to meet his or her individual or organizational requirements.

Claims 1 and 16 are directed to the broad process for screening cookie files in a client machine by using a list of cookie file sources that is maintained by a server (e.g., the professional service referred to above that maintains a universal reference source) and downloaded to the client machine. Claims 7, 12, 22 and 27 are directed to a process for user editing of the list. Neither of the applied references disclose or suggest either of these claimed processes.

ii. Walker

Walker discloses a browser that is capable of accessing only web pages previously authorized by a parent or supervisor of a user of the browser. In a supervisor mode of operation, a parent can browse through any accessible web site and continually add approved web sites to a database of authorized web sites. Later, in a user mode of operation, the child is capable of accessing only those web sites that have been added to the authorized web site database. As described on column 11, lines 25-36 of Walker, the database of authorized web sites may be pre-populated with an initial pre-approved list of child-appropriate URL's that are downloaded from a remote server. The parent can then manually add more web sites to the list.

Numerous other previously applied references disclose downloading lists of child-safe websites. See, for example, the Norton Internet Security 2000 ("NIS 2000") Black web site list discussed on page 3 of the Response filed April 11, 2006 (mail date of April 6, 2006). As previously argued, this is not Applicants' invention because a list of web sites is not a list of cookie file sources. In fact, a list of web sites might not include any cookie file sources. Furthermore, the purpose of downloading a list of web sites is different than the purpose of downloading a list of cookie file sources. The purpose of downloading a list of web sites, as described in Walker or NIS 2000 is to allow users to block access to such sites. The purpose of downloading a list of cookie file sources, in one preferred embodiment of the present invention, is to prevent certain cookie files from becoming stored on a user machine, or to delete such cookie files if they were previously stored. Access to the website associated with the cookie file is not necessarily blocked.

In the Final Rejection, the Examiner states that Walker discloses a client machine that requests a "list of sources" and a server that downloads a "list of sources" to the client machine. Throughout the entire prosecution history of this patent application, which has included seven Office Actions and a myriad of different prior art rejections, no prior art reference has been cited

that discloses or suggests any of steps (a)-(c) of claims 1 and 16, step (c) of claims 7 and 22, or step (a) of claims 12 and 27. In the Final Rejection, the Examiner admits that Walker does not disclose downloading a list of cookie file sources and relies instead upon Shrader for this limitation. However, as discussed below, Shrader also does not disclose downloading a list of cookie file sources, or steps (a)-(c) of claims 1 and 16, step (c) of claims 7 and 22, or step (a) of claims 12 and 27. Shrader thus fails to make up for the deficiencies in Walker and its equivalent prior art references.

iii. Shrader

Shrader discloses an improved cookie control process. Column 1, line 33 through column 2, line 19 of Shrader describes the problem in the art that is addressed, and reads as follows:

A web browser automatically stores certain user data during the process of the user browsing the Internet...

Another type of user data is a so-called "cookie." Because HTTP is a stateless protocol, a cookie can be set by a server to customize data to a particular user's web browser. Cookies thus provide a degree of "state" to HTTP. By default, a browser automatically stores cookie data without giving the user the option or knowledge of it being done. When a cookie is set as part of a HTTP transaction, it will include the path the cookie is valid for, the cookie's name and value, and other optional attributes, such as the expiration date for the cookie. In the prior art, a user can configure his or her web browser to show the cookie that the web server is attempting to set in a dialog box along with the options to set or cancel the cookie. After this initial display, the cookie value is unavailable for viewing or modification by the user. The browser may store cookie values in a text file, but this file can only be viewed outside of the browser and may only be updated when the browser is closed.

Thus, like basic authentication data, cookie data typically is not exposed to the user. Thus, for example, after a user has agreed to accept cookies, there is no easy way for the user to modify the cookie without first bringing down the browser.

It would be highly desirable to provide a web browser user with more control over what authentication and cookie data is stored on his or her behalf by a web browser or any other HTTP client application. The present invention addresses this problem.

Shrader provides a “cookie data display routine” to address this problem, as summarized on column 2, lines 48-67, which reads as follows (underlining added for emphasis):

The cookie display routine displays cookie data that is sent to the web browser from a given web server. The display routine places a cookie icon as part of the text and icons that remain visible above the web browser frame. The web browser displays a no-cookie icon if no cookies are set for the path. When the user selects the cookie icon, the browser displays a dialog box showing all the stored cookie values for the URL or path. A display in the dialog box shows the attributes of each cookie and scroll bars may be used to let the user browse all the values. Buttons at the bottom of the dialog box allow the user to delete or modify an existing cookie value. If desired, the cookie display routine could allow additional cookie values to be set. In addition, the cookie display routine could allow the user to view, edit, or delete all cookie values, not just ones for the current URL.

The cookie data display routine also enables a user to block all cookies from a particular site, such as a web server that returns nothing but advertisement graphics to subscribing URLs.

Shrader’s cookie data display routine is initiated only when a user (client machine) attempts to retrieve a specific URL via a web browser. That is, Shrader’s routine is initiated during a normal web surfing session and not as part of a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving at a client machine a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27). While Shrader arguably discloses “cookie file source(s)” in column 2, lines 64-67 as highlighted by the Examiner at the bottom of page 2 of the Final Rejection, and as underlined above, this reference to cookie file sources has nothing whatsoever to do with a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27). Accordingly, one cannot simply swap out Walker’s downloaded list of URL’s for Shrader’s cookie file sources as asserted in the Final Rejection because Shrader’s cookie file sources are not downloaded in the same manner or for the same purpose as Walker’s list of URL’s.



In the Final Rejection, the Examiner also highlights column 7, lines 10-15 and 30-35 of Shrader, as well as the Cookie Table referred to in Fig. 7, step 405 of Shrader. However, these portions of Shrader merely confirm that Shrader's cookie control process is initiated only when a user (client machine) attempts to retrieve a specific URL via a web browser, and that Shrader's cookie control process has nothing whatsoever to do with a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27).

Referring to Fig. 7 of Shrader, the first two steps are as follows:

1. Step 400: Wait for user input
2. Step 403: Decide if user is attempting to retrieve a URL with the web browser.

These steps clearly confirm that the subsequent steps, including step 405, occur only when a user is surfing the web.

Furthermore, Shrader's scheme fails to address one of the purposes of Applicants' invention, as highlighted on page 2, lines 19-30 of the present specification (excerpted above) namely, to screen cookie files in a client machine by using a list of cookie file sources that is maintained by a server and downloaded to the client machine (claims 1 and 16), and to allow for user editing of the list (claims 7, 12, 22 and 27). Shrader's scheme requires the user to be responsible for cookie management by making all of the decisions regarding which cookie files should be blocked and which cookie files should be allowed. For example, in step 407 of Fig. 7 in Shrader, if a user tags a cookie to be blocked, the browser will not send the cookie back to the web site, thereby disrupting the process that the cookie is meant to control. One of the purposes of the present invention is to allow a service provider to provide the bulk of cookie management with the user optionally assisting in the process via a personal trustlist and personal blacklist. Shrader does not disclose or suggest any such arrangement. Instead, Shrader puts the burden of cookie management on users, most of whom have no sophisticated knowledge base to draw upon for making sound decisions regarding cookie management.

Since steps (a) and (b) of claims 1 and 16 are not disclosed or suggested by the applied combination, step (c) of claims 1 and 16 inherently cannot be met by the applied combination.

iv. Walker in view of Shrader

Shrader is directed to a completely different problem in the art as Walker. However, Shrader and Walker appear to be compatible references. The combination of Walker and Shrader would provide a web site blocking tool that would also allow a user to provide enhanced cookie control for the web sites that are not blocked by Walker's process. Such a combination, however, would still not disclose or suggest the claimed invention.

B. Summary of claim limitations in claims 1, 7, 12, 16, 22 and 27 that are not disclosed or suggested by Walker in view of Shrader

For at least the reasons discussed above, none of the references applied against the independent claims disclose or suggest at least the following underlined limitations:

1. A method of screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the method comprising:

(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;

(b) downloading the list of cookie file sources from the server to the client machine; and

(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:

(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;

(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;

(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and

(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:

(a) receiving at the client machine, from a service provider, a master list of cookie file sources;

(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and

(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

16. An article of manufacture for screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;

(b) downloading the list of cookie file sources from the server to the client machine; and

(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

22. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;

(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;

(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and

(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

27. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) receiving at the client machine, from a service provider, a master list of cookie file sources;

(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and

(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

Furthermore, the unique combination of steps (a)-(c) in claims 1 and 16; steps (a)-(d) in claims 7 and 22; and steps (a)-(c) in claims 12 and 27 are not disclosed or suggested by the applied references.

In view of the above remarks, claims 1, 7, 12, 16, 22 and 27 are believed to be patentable over Walker in view of Shrader.

C. Patentability of dependent claims 2, 4-6, 8-11, 13-15, 17, 19-21, 23-26 and 28-30 over Walker in view of Shrader; and  
Patentability of dependent claims 3 and 18 over Walker in view of Shrader and NIS 2000

The dependent claims are believed to be patentable over the applied references for at least the reason that they are dependent upon allowable base claims and because they recite additional patentable elements and steps.

Regarding dependent claims 3 and 18, NIS 2000 does not make up for any of the above-highlighted deficiencies in Walker or Schrader.

D. Applicants' arguments do not stand or fall based on application of the CAFC's nonobviousness doctrine using a motivation/suggestion/teaching test

According to this CAFC test, when various pieces of prior art each contain elements of an invention, the prior art can be combined together to invalidate a patent on the invention only when there is some motivation, suggestion, or teaching to combine the prior art. The U.S. Supreme Court has granted a *writ of certiorari* in KSR International Co. v. Teleflex Inc. (Fed. Cir. 2006) to decide if the CAFC's motivation/suggestion/teaching test is legally correct in view of Supreme Court precedent. Commentators expect the Supreme Court to decide if the CAFC test is consistent with the Supreme Court's test in Sakraida v. Ag Pro, Inc. 425 U.S. 273 (1976). In Sakraida, the arrangement of old elements with each performing the same function it had been known to perform in the prior art was deemed to be not patentable, even though the novel arrangement perhaps produces a more striking result than in previous combinations. Sakraida is considered to be a case where patentability of a new combination was denied, even though there was no explicit motivation, suggestion, or teaching to combine the old elements.

Here, patentability of the claimed invention does not rely solely upon the motivation/suggestion/teaching test because the combination of references still lacks any

disclosure of at least steps (a) and (b) of claims 1 and 16, step (c) of claims 7 and 22, and step (a) of claims 12 and 27. Accordingly, these claims are believed to be patentable even under the Supreme Court's test in Sakraida, and regardless of whether the Supreme Court repudiates the CAFC's motivation/suggestion/teaching test.

E. Conclusion

For the reasons set forth above, Appellants respectfully submit that pending claims 1-30 are patentable over the prior art applied by the Examiner. Reversal of the rejections and issuance of a Notice of Allowance are respectfully requested at the earliest opportunity.

## VIII. APPENDIX OF CLAIMS

1. A method of screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the method comprising:

- (a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;
- (b) downloading the list of cookie file sources from the server to the client machine; and
- (c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

2. The method of claim 1, further comprising:

- (d) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine;
- (e) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine; and
- (f) modifying the downloaded list in accordance with the first and second exception lists.

3. The method of claim 1, further comprising:

- (d) receiving updates of the downloaded list from the server on a periodic basis.

4. The method of claim 1, further comprising:

- (d) displaying a message at the client machine indicating that a cookie file received from a cookie file source on the downloaded list has been detected.

5. The method of claim 1, further comprising:

(d) removing detected cookie files stored in the client machine.

6. The method of claim 1, further comprising:

(d) preventing detected cookie files from being stored in the client machine.

7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:

(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;

(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;

(c) receiving at the client machine, from a service provider, a master list of cookie file sources;  
and

(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

8. The method of claim 7, wherein the composite list is stored in the client machine independent of the first exception list, the second exception list and the received master list.

9. The method of claim 7, further comprising:

(e) receiving updates of the master list from the service provider on a periodic basis.

10. The method of claim 7, further comprising:

(e) removing stored cookie files received at the client machine from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources.

11. The method of claim 7, further comprising:

(e) preventing cookie files received at the client machine from cookie file sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list and, preventing storage of any received cookie files that have matching cookie file sources.

12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:

(a) receiving at the client machine, from a service provider, a master list of cookie file sources;  
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and  
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

13. The method of claim 12, wherein the master list and the composite list are stored



independently in the client machine.

14. The method of claim 12, further comprising:

(d) removing cookie files stored in the client machine and received from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

15. The method of claim 12, further comprising:

(d) preventing cookie files received at the client machine from sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list, and preventing storage of any received cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

16. An article of manufacture for screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;

(b) downloading the list of cookie file sources from the server to the client machine; and

(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

17. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine;

(e) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine; and

(f) modifying the downloaded list in accordance with the first and second exception lists.

18. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) receiving updates of the downloaded list from the server on a periodic basis.

19. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) displaying a message at the client machine indicating that a cookie file received from a cookie file source on the downloaded list has been detected.

20. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) removing detected cookie files stored in the client machine.

21. The article of manufacture of claim 16, wherein the computer-executable instructions

perform a method further comprising:

(d) preventing detected cookie files from being stored in the client machine.

22. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;

(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;

(c) receiving at the client machine, from a service provider, a master list of cookie file sources;

and

(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

23. The article of manufacture of claim 22, wherein the composite list is stored in client machine independent of the first exception list, the second exception list and the received master list.

24. The article of manufacture of claim 22, wherein the computer-executable instructions perform a method further comprising:

(e) receiving updates of the master list from the service provider on a periodic basis.

25. The article of manufacture of claim 22, wherein the computer-executable instructions

perform a method further comprising:

(e) removing stored cookie files received at the client machine from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources.

26. The article of manufacture of claim 22, wherein the computer-executable instructions perform a method further comprising:

(e) preventing cookie files received at the client machine from cookie file sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list and, preventing storage of any received cookie files that have matching cookie file sources.

27. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) receiving at the client machine, from a service provider, a master list of cookie file sources;

(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and

(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

28. The article of manufacture of claim 27, wherein the master list and the composite list are stored independently in the client machine.

29. The article of manufacture of claim 27, wherein the computer-executable instructions perform a method further comprising:

(d) removing cookie files stored in the client machine and received from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

30. The article of manufacture of claim 27, wherein the computer-executable instructions perform a method further comprising:

(d) preventing cookie files received at the client machine from sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list, and preventing storage of any received cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

## **IX. APPENDIX OF EVIDENCE**

A copy of a § 1.131 Declaration filed April 6, 2007 (entered on April 11, 2006) is attached as Evidence Appendix A and a copy of a 1.131 Declaration filed November 9, 2006 is attached as Evidence Appendix B. These Declarations were submitted to overcome a rejection over Buck '912. These Declarations were considered by the Examiner in the Office Actions dated May 15, 2006 and November 21, 2006. As discussed above, in a telephone call on December 7, 2006, the Examiner clarified that the § 102(e) rejection over U.S. Patent Application Publication No. 2002/0055912 (Buck) was withdrawn in the November 21, 2006 Office Action.

Regarding 37 CFR § 41.37(c)(ix), these Declarations were not “relied upon by appellant in the appeal” because the Examiner withdrew the rejection over Buck. However, these Declarations are being provided because they were requested in the “Order Returning Undocketed Appeal to the Examiner.”

**COPY**

Evidence Appendix A

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, ON THE DATE INDICATED BELOW.

BY:

*Gladys Morales*

Date:

*April 4, 2006*

MAIL STOP AMENDMENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In Re Patent Application of:  
Adam R. Schran et al.

Conf. No.: 3079

:  
:  
:  
Group Art Unit: 2161

Appln. No.: 09/820,054

:  
Examiner: Etienne Pierre Leroux

Filing Date: March 28, 2001

:  
Attorney Docket No.: 10397-1U1

Title:

SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND  
LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA

**DECLARATION OF PRIOR INVENTION  
TO OVERCOME CITED PATENT (37 CFR § 1.131)**

**PURPOSE OF DECLARATION**

This declaration is being submitted to establish completion of the invention in this application in the United States at a date prior to October 20, 2000, which is the earliest possible effective date of the prior art U.S. Patent Application Publication No. 2002/0055912 (Buck), which was cited and applied by the Examiner in an Office Action dated November 18, 2005.

The persons making this declaration are the inventors, and are thus qualified to submit this declaration under 37 CFR § 1.131.

### **FACTS AND DOCUMENTARY EVIDENCE**

To establish the date of completion of the invention of this patent application, copies of the following documents and supporting statements are submitted as evidence:

#### Documents

EXHIBIT 1: Screen shot printout of a file folder that contains the executable code (.exe) of a beta version of ActivePrivacy.

EXHIBIT 2: Document entitled "INTELLECTUAL PROPERTY NEEDS ASSESSMENT" which provides an overview of the technical capabilities of ActivePrivacy.

EXHIBIT 3: Patentability search memorandum.

EXHIBIT 4: Email from a customer of ActivePrivacy.

EXHIBIT 5: Chart of independent claim limitations that shows documentation for each claim limitation.

#### Supporting statements

1. The blacked out dates labeled as D1-D4<sup>1</sup> in Exhibit 1 are all prior to October 20, 2000.
2. The blacked out date labeled D1 in Exhibit 2 is prior to October 20, 2000.
3. The blacked out dates labeled D1 and D2 in Exhibit 3 are both prior to October 20, 2000.
4. The blacked out dates labeled D1 and D2 in Exhibit 4 are both prior to October 20, 2000.
5. Each claim limitation in Exhibit 5 is supported by documentation that is dated prior to October 20, 2000. Text portions T1-T6 (there is no T2) referred to in Exhibit 5 correspond to respectively labeled text portions in Exhibits 2 and 3.
6. A beta version of ActivePrivacy was created and released prior to October 20, 2000, as evidenced by Exhibits 1 and 2. See, text portion T7 of Exhibit 2.
7. A commercial subscription-based version of ActivePrivacy was released and made available for a license fee prior to October 20, 2000, as evidenced by Exhibit 4.

---

<sup>1</sup> D4 refers only to the 272 kB ActivePrivacy.exe file.



8. The beta and commercial version of ActivePrivacy both contained all of the functionality of the claim limitations shown in Exhibit 5. General descriptions of such functionality are given in Exhibits 2 and 3.

9. ActivePrivacy is the commercial name of a software product associated with the presently claimed invention, as further evidenced by Figs. 4 and 6 of the present invention which show screen shots labeled with "ActivePrivacy."

From the attached documents and the supporting statements, we submit that it has been established that the invention in this application was made prior to October 20, 2000, which is the earliest possible effective date.

#### **TIME OF PRESENTATION OF THE DECLARATION**

This declaration is submitted prior to final rejection.

#### **DECLARATION**

As a person signing below:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Application No. 09/820,054

Reply to Office Action of November 18, 2005 -- "Declaration of Prior Invention..."

### SIGNATURES

Full name of first or  
sole inventor

Adam R. Schran

Inventor's Signature

Date

4/5/2006

Residence

Philadelphia, Pennsylvania

Citizenship

United States of America

Post Office Address

217 Church St #4 Phila PA 19147

Full name of second  
joint inventor

Robert E. Darlington

Inventor's Signature

Date

Residence

Los Alamos, New Mexico

Citizenship

United States of America

Post Office Address

3260-B Orange Street, Los Alamos, New Mexico 87544

**SIGNATURES**

Full name of first or  
sole inventor Adam R. Schran

Inventor's Signature

Date

Residence Philadelphia, Pennsylvania

Citizenship United States of America

Post Office Address

Full name of second  
joint inventor Robert E. Darlington

Inventor's Signature

Date

Residence Los Alamos, New Mexico

Citizenship United States of America

Post Office Address 3260-B Orange Street, Los Alamos, New Mexico 87544

EXHIBIT 1 of "Declaration of Prior Invention..."  
(Application No. 09/820,054)

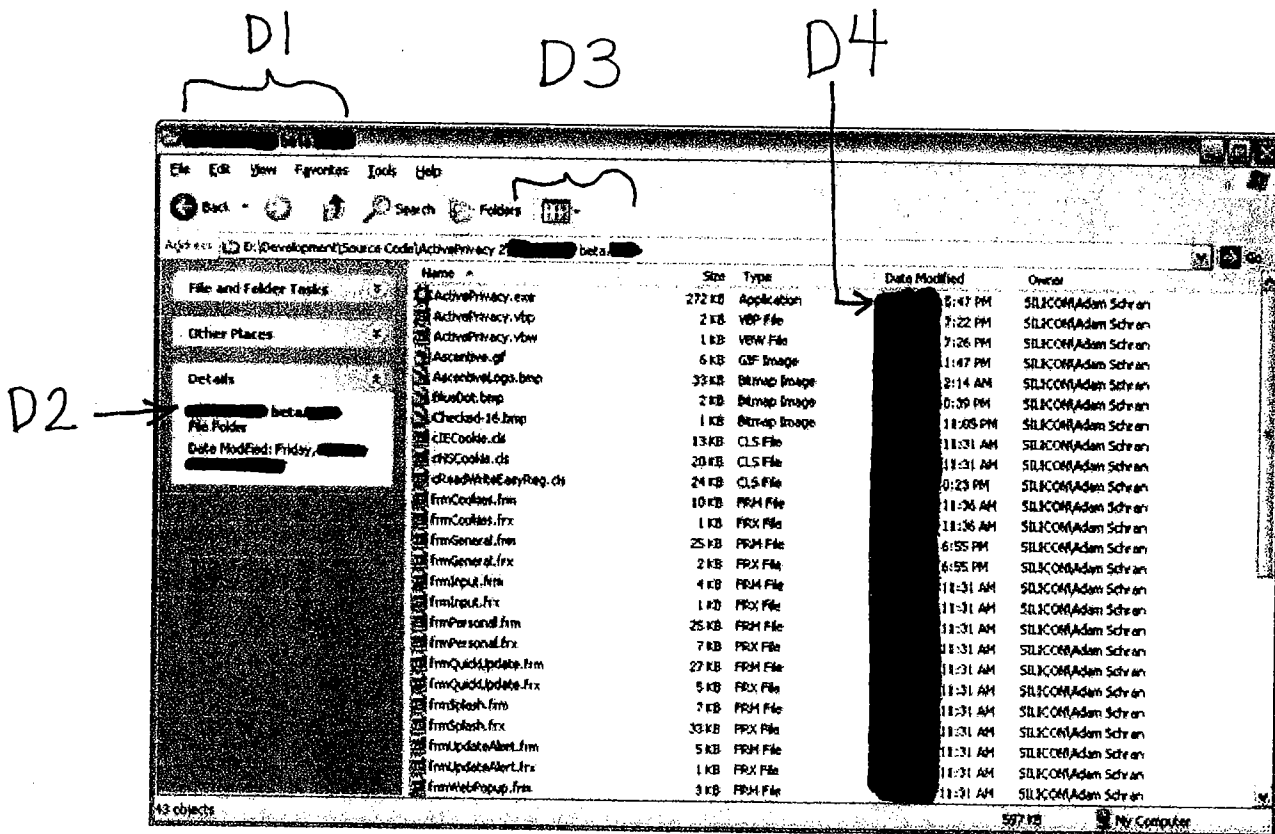


EXHIBIT 2 of "Declaration of Prior Invention..."  
(Application No. 09/820,054)

INTELLECTUAL PROPERTY NEEDS ASSESSMENT

Adam Schran



**Introduction**

Ascentive, an Internet software company, was founded in November 1998 on the proverbial 'back of the napkin' and launched in January 1999. Since then, revenue has grown at an average 50% per month, resulting from a successful focus on building a network of 3,000+ affiliate web sites to bootstrap the company.

**Products**

Since launch, Ascentive has brought to market two consumer software products for Windows:

- WebROCKET Internet Optimizer – An instant speed boost for any dial-up or high-speed Internet connection.
- WinROCKET Computer Optimizer – Performance booster for all computers running Windows 95 and 98.

**ActivePrivacy Overview**

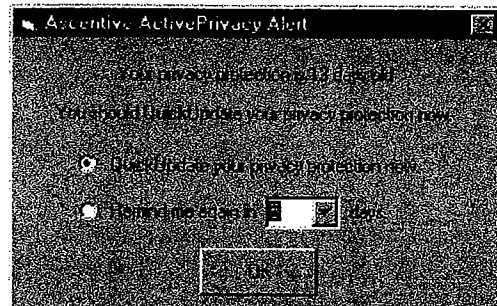
ActivePrivacy, currently undergoing beta testing, represents a leap forward in privacy protection from the current tools-driven convention to a service-driven model.

In the current schema, Internet users have one of three options:

- Head in the sand: Do nothing about potential privacy violations.
- Scorched earth: Disable all avenues for privacy violations, thus reducing the utility and automation of many web sites.
- Do it yourself: Scan for potential privacy violations yourself, consuming time and energy.

ActivePrivacy's service approach is superior to all three methods.

- Customer subscribes to the ActivePrivacy QuickUpdate privacy service to manage their privacy needs. The QuickUpdate service includes the latest privacy protection, consisting of a "Watchlist" of sites that use cookie files to store unique or identifying information.
- ActivePrivacy, the client software, scans for privacy violations and takes corrective action while you use the Internet. To trigger potential privacy violations, the Watchlist (retrieved by the client software from Ascentive's QuickUpdate server) is merged with the end user's Blacklist, exempting any sites in the end user's Trustlist.
- The end user is reminded to keep their Watchlist up to date by QuickUpdating frequently.



**Inventions**

We believe the following innovations in ActivePrivacy are new and non-obvious, and are good candidates for patent protection.

- Determining and taking corrective action for privacy violations that have already occurred by merging "QuickUpdate" Watchlist privacy protection with the end-user's Blacklist and Trustlist.
- "Privacy safe browsing", a browser window in the client/server that uses the QuickUpdate privacy protection to preemptively strike against privacy violations.
- The ActivePrivacy QuickUpdate server, a system that distributes incremental updates to end users' privacy protection through the QuickUpdate client software.

**AKIN, GUMP, STRAUSS, HAUER & FELD, L.L.P.**

ATTORNEYS AT LAW  
One Commerce Square - 2005 Market Street - Suite 2200  
PHILADELPHIA, PA 19103-7086  
Telephone: (215) 965-1200 - FAX: (215) 965-1210  
E-MAIL: &@@akingump.com

CONFIDENTIAL

D1 → [REDACTED]

CONFIDENTIAL

VIA FACSIMILE: 703-415- 1017 - (Confirmation copy via First-Class Mail)

SEARCHER: Randy Lacasse

Client No.:

210397.0001

FROM: Louis Sickles

PAGE 1 OF 4

DEADLINE:

D2 → [REDACTED]

☐ Telephone Confirmation

☒ New Instructions

☐ Fax Confirmation

INSTRUCTIONS:

☐ Detailed Instructions Attached

Please conduct a patentability search on a regular basis for a Method of  
Expunging Unwanted Cookies from a Computer.

A "cookie" is a short piece of data which is transmitted from certain Internet  
hypertext transfer protocol (HTTP) server computers to a client computer when the HTTP server  
connects to the client computer in response to a uniform resource locator (URL) request from the  
client computer. The cookie includes, in part, data related to the web page accessed by the client  
computer and the domain attributes of the server. Cookies transmitted from individual server  
computers are separately stored in the memory of the client computer.

In subsequent transactions between the client computer and a server which had  
previously transmitted a cookie to the client computer, (or a server included in the domain  
specified by the server), a copy of the cookie stored in the client computer and linked to that  
domain address is automatically included in the client computer's URL request. In this way, the  
server receiving the URL request knows that the user has previously connected to the server and  
can (if desired) direct the client's access to a specific page (or pages) on its web site.

Cookies are typically used by Internet shopping sites to keep track of the user's  
shopping cart. When a user first visits an Internet shopping site, the user is sent a cookie  
containing the name (ID number) of a shopping cart. Each time an item is selected for purchase,  
the shopping site correlates that selection to the shopping cart by the shopping cart ID number

contained in the cookie and adds the selection to the cookie. When the user is done with shopping, the checkout page lists all of the items in the shopping cart tied to the cookie. Without cookies, the user would have to keep track of all the items that the user wanted to buy and type them into the checkout page at the conclusion of the transaction, or buy each item one at a time. Alternative to accumulating the shopping cart data in a single cookie, the shopping site could send a separate cookie containing the selected item number to the client computer whenever an item was selected to purchase.

One of the less admirable and controversial uses of cookies is for tracking the browsing and buying habits of individual web users. On a single web site or a group of web sites within a single sub-domain, cookies can be used to see what web pages the user visits and how often the user visits them. On web sites which display banner advertisements from a single marketing site, cookies can be used to track the browsing habits on all of the web sites being serviced by the marketing site. Tracking is accomplished by issuing a cookie with the marketing site's domain specified when the user clicks on the advertisement. Subsequent connection of a user to any web site displaying one of the marketing site's advertisements results in a cookie being sent to the marketing site. The marketing site can correlate the users buying habits from the plurality of cookies and develop a profile of the user.

Currently, a user has only two options if the user prefers not to have his web browsing habits tracked. Commercial browsers, (e.g., Internet Explorer or Netscape Navigator), provide options that: (1) prevent any cookie from being stored in the user's computer, (2) notify the user each time a cookie is sent to the browser allowing the user to reject or accept the cookie, or (3) accept all cookies. None of the aforementioned options is entirely satisfactory. In the first case, the user will be prevented from connecting with many desirable sites that do not abuse the use of the cookie. In the second case, the user will be likely be annoyed by the notification messages which may occur numerous times during a connection to a single web site.

Software applications are known which can be installed in a client computer to give the user additional control over cookies. These software packages typically allow the user to accept, reject or delete cookies from the client computer that originate from user specified web sites. However, all of these known software packages require the user to develop the list of unwanted web sites.

In the proposed system concept an HTTP server maintains a watch list of Internet sites that use cookies to store unique or identifying information about a user. The user's computer contains both a user developed black list of Internet sites for which the user prefers not to have cookies stored in his system, and a user developed list of trusted Internet sites for which the user has perfect trust. In use, the user is periodically prompted to connect the client computer with the HTTP server containing the watch list. In response, the HTTP server downloads the watch list to the user's computer. The watch list is combined with the user's blacklist and the user's trusted list to create a composite list of Internet sites. The composite list is formed by subtracting sites on the trusted list from the watch list and adding the result to the user's black list.

T1 {  
T4 {  
T5  
T6  
T4  
T5

The user's software can operate in two different modes. In the first mode, the user's software deletes offending cookies from the user's memory based on the composite list. In this mode, the user may set the software to execute at any periodicity he chooses, from seconds to hours. In the second mode, the software operates continuously to intercept cookies as the cookies are received from the offending web server. The watch list may also include attributes that characterize the Internet sites using cookies based on the degree of identifying information contained in the cookie. In these instances, the user would be notified that the cookie was present in his system or is being sent to the system and the user would be given the option of editing the composite list to accept or reject cookies from that site.

T3 {

Note that a similar concept is used to download anti-virus software to client computers. However, the concept of the present invention differs in at least two respects: (1) the combining of the watch list, the black list and the trusted list and (2) the concept of detecting and rejecting the cookie as it is received by the user's computer.

The following words and phrases are sometimes used synonymously for cookies and may assist in searching for references related to "cookies": persistent cookie; token; state object; and state management.

In summary, please focus your search on the following concepts: (1) a computer software program residing in a server computer that maintains a watch list of computer servers that use cookies to store unique or identifying information about a user and upon request downloads the watch list to a subscribing client computer; and (2) a computer program that resides in a subscribing client computer that maintains a black list and a trusted list and uses the



black list and the trusted list in conjunction with the downloaded watch list to either delete unwanted cookies from the client computer memory and/or reject unwanted cookies as they are received in the client computer.

If you require additional information please contact me at the above 215-965-1294.

Thank you.

---

---

**FOR SEARCHER'S USE ONLY**

Date Completed: \_\_\_\_\_

Time: \_\_\_\_\_

Costs: \_\_\_\_\_

EXHIBIT 4 of "Declaration of Prior Invention..."  
(Application No. 09/820,054)

D1

CSNavy@aol.com, 01:53 AM [REDACTED], Active Privacy Problem

Page 1 of 1

D2

From: CSNavy@aol.com  
Date: Sat, [REDACTED] 02:53:25 EDT  
Subject: Active Privacy Problem  
To: comments@ascentive.com  
X-Mailer: AOL 5.0 for Windows sub 119

Dear Sir Or Madam:

After the first few days of using ActivePrivacy I've been unable to keep the program running on my computer. After 20 minutes to 1 hour a window pops up with Run error Division by zero and the program shuts down once this is acknowledged.

This makes the ActivePrivacy program virtually useless to me. Unless I can find a solution to this I will discontinue using it and uninstall this program.

V/R  
Kelsey Baker

A11

**EXHIBIT 5 of "Declaration of Prior Invention..."**  
(Application No. 09/820,054)

**Chart of independent claim limitations that shows documentation for each claim limitation**

Text of independent claims	Exhibit(s) that support claim limitations
1. A method of screening cookie files in a client machine, the method comprising:	
(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;	Exhibit 2: T1 Exhibit 3: T1
(b) downloading the list from the server to the client machine; and	Exhibit 2: T1 Exhibit 3: T1
(c) using the downloaded list to detect cookie files received at the client machine from sources on the downloaded list.	Exhibit 2: T3 Exhibit 3: T3
16.	Same as claim 1

Text of independent claims	Exhibit(s) that support claim limitations
7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) creating a first exception list including the identity of sources that are permitted to store cookie files in the client machine;	Exhibit 2: T4 Exhibit 3: T4
(b) creating a second exception list including the identity of sources that are not permitted to store cookie files in the client machine;	Exhibit 2: T5 Exhibit 3: T5
(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and	Exhibit 2: T1 Exhibit 3: T1
(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.	Exhibit 2: T6 Exhibit 3: T6
22.	Same as claim 7

Text of independent claims	Exhibit(s) that support claim limitations
12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) receiving at the client machine, from a service provider, a master list of cookie file sources;	Exhibit 2: T1 Exhibit 3: T1
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and	Exhibit 2: T4, T6 Exhibit 3: T4, T6
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.	Exhibit 2: T5, T6 Exhibit 3: T5, T6
27.	Same as claim 12

COPY  
Evidence Appendix B

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In Re Patent Application of: :  
Adam R. Schran et al. :  
 :  
Conf. No.: 3079 : Group Art Unit: 2161  
 :  
Appln. No.: 09/820,054 : Examiner: Etienne Pierre Leroux  
 :  
Filing Date: March 28, 2001 : Attorney Docket No.: 10397-1U1  
 :  
Title: SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND  
LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA

**SUPPLEMENTAL DECLARATION OF PRIOR INVENTION**  
**TO OVERCOME CITED PATENT (37 CFR § 1.131)**

**PURPOSE OF DECLARATION**

This supplemental declaration is being submitted to establish completion of the invention in this application in the United States at a date prior to October 20, 2000, which is the earliest possible effective date of the prior art U.S. Patent Application Publication No. 2002/0055912 (Buck), which was cited and applied by the Examiner in Office Actions dated November 18, 2005 and May 15, 2006.

The persons making this declaration are the inventors, and are thus qualified to submit this declaration under 37 CFR § 1.131.

### **FACTS AND DOCUMENTARY EVIDENCE**

To establish the date of completion of the invention of this patent application, copies of the following documents and supporting statements are submitted as evidence:

#### Documents

REVISED EXHIBIT 5: Chart of currently pending independent claim limitations that shows documentation for each claim limitation.

#### Supporting statements

1. Each claim limitation in Exhibit 5 is supported by documentation that is dated prior to October 20, 2000. Text portions T1-T6 (there is no T2) referred to in Exhibit 5 correspond to respectively labeled text portions in Exhibits 2 and 3 of the originally filed § 1.131 Declaration.

2. The beta and commercial version of ActivePrivacy both contained all of the functionality of the claim limitations shown in Exhibit 5. General descriptions of such functionality are given in Exhibits 2 and 3 of the originally filed § 1.131 Declaration.

From the attached documents and the supporting statements, and the documents and supporting statement in the originally filed § 1.131 Declaration, we submit that it has been established that the invention in this application was made prior to October 20, 2000, which is the earliest possible effective date of Buck.

### **TIME OF PRESENTATION OF THE DECLARATION**

This declaration is submitted prior to final rejection.

**DECLARATION**

As a person signing below:

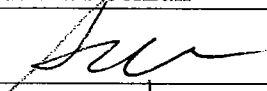
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**SIGNATURES**

Full name of first or  
sole inventor

Adam R. Schran

Inventor's Signature



Date

10/31/2006

Residence

Philadelphia, Pennsylvania

Citizenship

United States of America

Post Office Address

217 Church Street, #4, Philadelphia, Pennsylvania 19147

Full name of second  
joint inventor

Robert E. Darlington

Inventor's Signature

Date

Residence

Los Alamos, New Mexico

Citizenship

United States of America

Post Office Address

3260-B Orange Street, Los Alamos, New Mexico 87544

### DECLARATION

As a person signing below:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

### SIGNATURES

Full name of first or  
sole inventor Adam R. Schran

Inventor's Signature


Date

Residence Philadelphia, Pennsylvania

Citizenship United States of America

Post Office Address 217 Church Street, #4, Philadelphia, Pennsylvania 19147

Full name of second  
joint inventor Robert E. Darlington

Inventor's Signature 

Date 11/4/2006

Residence Los Alamos, New Mexico

Citizenship United States of America

Post Office Address 3260-B Orange Street, Los Alamos, New Mexico 87544



**EXHIBIT 5 of “Supplemental Declaration of Prior Invention...”**  
(Application No. 09/820,054)

**Chart of independent claim limitations that shows documentation for each claim limitation**

Text of independent claims	Exhibit(s) that support claim limitations
1. A method of screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the method comprising	
(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;	Exhibit 2: T1 Exhibit 3: T1
(b) downloading the list of cookie file sources from the server to the client machine; and	Exhibit 2: T1 Exhibit 3: T1
(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.	Exhibit 2: T3 Exhibit 3: T3
16.	Same as claim 1

Text of independent claims	Exhibit(s) that support claim limitations
7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;	Exhibit 2: T4 Exhibit 3: T4
(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;	Exhibit 2: T5 Exhibit 3: T5
(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and	Exhibit 2: T1 Exhibit 3: T1
(d) modifying the master list in accordance with the first and	Exhibit 2: T6

B5

06

second exception lists, wherein the composite list is the modified master list.	Exhibit 3: T6
22.	Same as claim 7

Text of independent claims	Exhibit(s) that support claim limitations
12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) receiving at the client machine, from a service provider, a master list of cookie file sources;	Exhibit 2: T1 Exhibit 3: T1
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and	Exhibit 2: T4, T6 Exhibit 3: T4, T6
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.	Exhibit 2: T5, T6 Exhibit 3: T5, T6
27.	Same as claim 12

## **X. APPENDIX OF RELATED DECISIONS**

None.

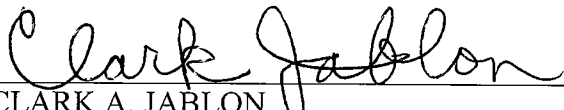
## **XI. OTHER MATERIAL THAT APPELLANT CONSIDERS NECESSARY OR DESIRABLE**

See the accompanying Supplemental Information Disclosure Statement that includes a citation for U.S. Patent No. 5,706,507 (Schloss).

During the telephone conversation of December 7, 2006, the Examiner stated that he located an additional reference (Schloss) after issuing the Final Rejection that he believes should be formally applied against the claims. Applicants have carefully reviewed Schloss and do not believe that it is any more relevant to the presently claimed invention than the current prior art of record. Schloss does not disclose any of the above-highlighted (underlined) limitations in the independent claims.

Respectively submitted,

Adam R. Schran *et al.*

December 13, 2007 By:   
(Date) CLARK A. JABLON  
Registration No. 35,039  
AKIN GUMP STRAUSS HAUER & FELD LLP  
One Commerce Square  
2005 Market Street, Suite 2200  
Philadelphia, PA 19103-7013  
Telephone: 215-965-1200  
Direct Dial: 215-965-1293